02115102

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

COMMUNICATION OF
INTERNATIONAL APPLICATIONS

(PCT Article 20)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE
in its capacity as designated Office

Date of mailing:
31 January 2002 (31.01.02)

The International Bureau transmits herewith copies of the international applications having the following international application numbers and international publication numbers:

International application no.:	International publication no.:
PCT/JP01/06298	

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra
Telephone No.: (41-22) 338.83.38

US

特　許　協　力　条　約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　PH-1237-PCT	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０１／０６２９８	国際出願日 （日.月.年）　１９．０７．０１	優先日 （日.月.年）　２４．０７．００
出願人（氏名又は名称） 高取　直		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　2　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　1　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査[redacted]

国際出願番[redacted]PCT／JP01／06298

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／00, G09C1／00, H04L12／22, H04L12／58

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／00, G09C1／00, H04L12／22, H04L12／58

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	EP 779727 A (NIPPON TELEGRAPH AND TELEPHON CORPORATION) 18.6月.1997(18.06.97), 第6欄第6行-第12欄第54行 & JP 9-321750 A & US 5757922 A	1-6
Y	JP 2000-59355 A (大日本印刷株式会社) 25.2月.2000(25.02.00), 第2欄第4行-第4欄第10行 (ファミリーなし)	1-6
Y	JP 10-301489 A (大成建設株式会社) 13.11月.1998(13.11.98), 第3欄第4-33行 (ファミリーなし)	1-6

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 03. 08. 01	国際調査報告の発送日 14.08.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正 5M 9364 電話番号 03－3581－1101 内線 3597

様式PCT／ISA／210（第2ページ）（1998年7月）

記録原本

特許協力条約に基づく国際出願願書
原本（出願用）- 印刷日時 2001年07月19日（19.07.2001）木曜日 14時15分48秒

PH-1237-PCT

0	受理官庁記入欄	
0-1	国際出願番号.	PCT/JP01/06298
0-2	国際出願日	19.07.01
0-3	(受付印)	PCT International Application 日本国特許庁
0-4	様式-PCT/RO/101 この特許協力条約に基づく国際出願願書は、	
0-4-1	右記によって作成された。	PCT-EASY Version 2.92 (updated 01.03.2001)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁（RO/JP）
0-7	出願人又は代理人の書類記号	PH-1237-PCT
I	発明の名称	電文送信装置及び電文受信装置
II	出願人	
II-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
II-2	右の指定国についての出願人である。	~~米国のみ（US only）~~ すべての指定国（all designated States）
II-4ja	氏名(姓名)	高取 直
II-4en	Name (LAST, First)	TAKATORI, Sunao
II-5ja	あて名:	155-0031 日本国 東京都 世田谷区 北沢三丁目５番１８号 株式会社鷹山内
II-5en	Address:	c/o Yozan Inc., 5-18, Kitazawa 3-chome, Setagaya-ku, Tokyo 155-0031 Japan
II-6	国籍（国名）	日本国 JP
II-7	住所（国名）	日本国 JP
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-1-2	右の指定国についての出願人である。	~~米国のみ（US only）~~ すべての指定国（all designated States）
III-1-4ja	氏名(姓名)	清松 久典
III-1-4en	Name (LAST, First)	KIYOMATSU, Hisanori
III-1-5ja	あて名:	155-0031 日本国 東京都 世田谷区 北沢三丁目５番１８号 株式会社鷹山内
III-1-5en	Address:	c/o Yozan Inc., 5-18, Kitazawa 3-chome, Setagaya-ku, Tokyo 155-0031 Japan
III-1-6	国籍（国名）	日本国 JP
III-1-7	住所（国名）	日本国 JP

特許協力条約に基づく国際出願願書 PH-1237-PCT

原本（出願用）- 印刷日時 2001年07月19日（19.07.2001）木曜日 14時15分48秒

IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人（agent）
IV-1-1ja	氏名(姓名)	平木 祐輔
IV-1-1en	Name (LAST, First)	HIRAKI, Yusuke
IV-1-2ja	あて名:	105-0001 日本国 東京都 港区 虎ノ門一丁目17番1号 虎ノ門5森ビル 3階
IV-1-2en	Address:	Toranomon No.5 Mori Building Third Floor, 17-1, Toranomon 1-chome Minato-ku, Tokyo 105-0001 Japan
IV-1-3	電話番号	03-3503-8637
IV-1-4	ファクシミリ番号	03-3503-0414
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)
IV-2-1ja	氏名	関谷 三男
IV-2-1en	Name(s)	SEKIYA, Mitsuo
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	--
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	US
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。	
V-6	指定の確認から除かれる国	なし（NONE）
VI-1	先の国内出願に基づく優先権主張	
VI-1-1	出願日	2000年07月24日（24.07.2000）
VI-1-2	出願番号	特願2000-222680号 ▲RO
VI-1-3	国名	日本国 JP
VI-2	優先権証明書送付の請求 上記の先の出願のうち、右記の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁に対して請求している。	VI-1
VII-1	特定された国際調査機関(ISA)	日本国特許庁（ISA/JP）

特許協力条約に基づく国際出願願書 PH-1237-PCT

原本（出願用）- 印刷日時 2001年07月19日（19.07.2001）木曜日 14時15分48秒

VIII	申立て	申立て数	
VIII-1	発明者の特定に関する申立て	-	
VIII-2	出願し及び特許を与えられる国際出願日における出願人の資格に関する申立て	-	
VIII-3	先の出願の優先権を主張する国際出願日における出願人の資格に関する申立て	-	
VIII-4	発明者である旨の申立て（米国を指定国とする場合）	-	
VIII-5	不利にならない開示又は新規性喪失の例外に関する申立て	-	
IX	照合欄	用紙の枚数	添付された電子データ
IX-1	願書（申立てを含む）	4	-
IX-2	明細書	9	-
IX-3	請求の範囲	2	-
IX-4	要約	1	abst1237.txt
IX-5	図面	6	-
IX-7	合計	22	
	添付書類	添付	添付された電子データ
IX-8	手数料計算用紙	✓	-
IX-9	個別の委任状の原本	✓	-
IX-17	PCT-EASYディスク	-	ﾌﾚｷｼﾌﾞﾙﾃﾞｨｽｸ
IX-18	その他	納付する手数料に相当する特許印紙を貼付した書面	-
IX-18	その他	国際事務局の口座へ振込を証明する書面	-
IX-19	要約書とともに提示する図の番号	1	
IX-20	国際出願の使用言語名:	日本語	
X-1	提出者の記名押印		
X-1-1	氏名(姓名)	平木 祐輔	
X-2	提出者の記名押印		
X-2-1	氏名(姓名)	関谷 三男	

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	19.07.01
10-2	図面：	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP

特許協力条約に基づく国際出願願書 PH-1237-PCT

10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	03 AUGUST 2001 (03.08.01)

明　細　書

電文送信装置及び電文受信装置

技術分野

本発明は、送信電文及びダミー電文を分割しかつそれらの順序を入れ替えて伝送することで、盗聴等による電文内容の把握を困難にした電文送信装置及び電文受信装置に関する。

背景技術

インターネットの普及により個人情報などの機密性の高い情報を電子メール等により送信する機会が増えている。インターネットはある情報を送る場合、そのデータをまずパケットに分割する。これら各パケットにはヘッダといわれる標識が付き、このヘッダに行き先やパケットを再度組み立てるときの順番などの情報が記されている。このヘッダのあるおかげで、たとえどこかの回線が断たれたとしても各パケットはいくつかの違う順路をたどって目的地に着くことができ、そこで元の通りに再構築され、正確な情報に再現される。この方式だと、１つの回線上をいくつもの行き先の異なったパケットが通過できるので、効率がきわめて良く、データ通信には優れた方式だといえる。

インターネットは各地域や学校・企業などの単位がもつネットワーク同士がつながっており、そのつなぎ目にあたるところにはルーターと呼ばれるコンピュータが介在する。ルーターは到着してくるパケットのヘッダを読み取って目的地へと再び送り出し、そのようなことが繰り返されてパケットは最終目的地にたどり着く。このようにデータ（情報）はインターネットにつながれたネットワークのルーターをリレー式に送られながら目的地にたどり着くので、このような情報伝達方式を称して「バケツリレー式」などといったりする。

パケット通信によっていくつもの中継地点を通過するため、その間でデータを盗聴される危険がある。そこで、データを安全に送受信するた

めに、各種の暗号方式が実用化されている。送信側で平文を解読が困難な暗号文に暗号化し、受信側で暗号文を平文に復号化するには多くのデータ処理が必要があり、暗号化／復号化のためのプログラムや送受信装置の構成が複雑になるとともに、処理能力の高いプロセッサが必要になることがある。

特開平９－１８４７３号公報には、ユーザデータ全てを暗号化して伝送するような高い処理能力を持たないプロセッサを使用して、単純な手法によりユーザデータを秘匿してデータ通信を行えるようにしたデータ伝送装置が記載されている。このデータ伝送装置は次のように構成されている。送信が要求されたユーザデータをサブユーザデータに分割し、送信するパケットデータ内で分割したサブユーザデータをランダムに再配置し、さらに、送信するパケットデータを故意にランダムな順序に並べ替える。そして、パケットデータ中の通信制御情報（ユーザデータ順序番号や送達確認情報や再送情報等）の固定長のデータを暗号化して送信する。受信側では、通信制御情報を復号化し、その中に含まれているユーザデータ順序番号に係るキー情報に基づいてユーザデータを復元する。

また、特許公開２０００－１２４８９１号公報には、暗号化された暗号化データとその暗号化のために用いられた暗号化方式とを同時に送信せずに、別個独立に時間差をもって送信することで、安全性の向上を期待するようにしたデータ送受信装置が記載されている。

発明の開示

しかしながら、上記特開平９－１８４７３号公報に記載されているデータ伝送装置においても通信制御情報を暗号化／復号化する必要があり、通信制御情報を暗号化／復号化するために多くのデータ処理が必要である。

本発明はこのような課題を解決するためになされたもので、簡易なデータ処理で第三者による電文内容の把握を困難にした電文送信装置及び電文受信装置を提供することを目的とする。

本発明の電文送信装置は、送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文をパケット通信方式で送信するデータ送信部と、を備える。

また、本発明の電文送信装置は、送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文を元の順序に戻すための制御情報を有する制御電文を生成する制御電文生成部と、前記電文順序並替部によって並べ替えられた送信電文及び前記制御電文生成部によって生成された制御電文をパケット通信方式で送信するデータ送信部と、を備える。

また、前記データ送信部は、前記電文順序並替部によって並べ替えられた送信電文と前記制御電文とを別に送信することで、第三者による電文解読をより困難なものにすることができる。

また、前記ダミー電文は、前記送信電文の内容と異なる内容であって、送信電文の内容の把握を妨げる内容であることで、送信電文の内容の把握をより困難なものにできる。

また、本発明の電文受信装置は、パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した電文を記憶する受信電文記憶部と、該受信電文記憶部に記憶されている電文からダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備える。

また、本発明の電文受信装置は、パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した受信電文を記憶する受信電文記憶部と、該データ受信部で受信した制御電文を記憶する制御電文記憶部と、前記受信電文記憶部に記憶されている電文から前記制御電文記憶部に記憶されている制御電文に基づいてダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備える。

本明細書は本願の優先権の基礎である特願２０００－２２２６８０の明細書および/または図面に記載される内容を包含する。

図面の簡単な説明

図１は本発明に係る電文送信装置及び電文受信装置のブロック構成図である。

図２は送信電文分割部及びダミー電文分割部の動作を示す図である。

図３は電文順序並替部の動作を示す図である。

図４は制御情報の例を示す図である。

図５はデータ送信部の動作を示す図である。

図６は電文復元部の動作を示す図である。

発明を実施するための最良の形態

以下、添付図面を参照しながら本発明の好適な実施の形態について詳細に説明する。

図１は、本発明に係る電文送信装置及び電文受信装置のブロック構成図である。電文送信装置１０は、送信電文を複数の電文に分割する送信電文分割部１１と、ダミー電文を複数の電文に分割するダミー電文分割部１２と、分割された送信電文及び分割されたダミー電文の順序を並べ替える電文順序並替部１３と、並べ替えられた送信電文を元の順序に戻すための制御情報を有する制御電文を生成する制御電文生成部１４と、並べ替えられた各分割電文及び制御電文をそれぞれパケット通信方式で送信するデータ送信部１５とからなる。

電文受信装置２０は、データ受信部２１と、受信した分割電文を一時記憶する受信電文記憶部２２と、受信した制御電文を一時記憶する制御電文記憶部２３と、制御電文に含まれている制御情報に基づいて並べ替えられた電文を元の順序に戻して電文を復元する電文復元部２４とからなる。

電文送信装置１０と電文受信装置２０とはインターネット３０等のオープンなネットワークを介して接続される。

図２は、送信電文分割部及びダミー電文分割部の動作を示す図である。ここでは送信電文及びダミー電文をそれぞれ８個の電文に分割する例を示している。送信電文分割部１１は、図２（ａ）に示す送信電文Ｓを、図２（ｂ）に示すように８個の電文Ｓ１～Ｓ８に分割する。ダミー電文分割部１２は、図２（ｃ）に示すダミー電文Ｄを、図２（ｄ）に示すように８個の電文Ｄ１～Ｄ８に分割する。なお、分割するバイト数は任意であり、各分割部毎にそのバイト数が異なっていてもよい。

図３は、電文順序並替部の動作を示す図である。電文順序並替部１３は、図３（ａ）に示すように、分割された各電文Ｓ１～Ｓ８，Ｄ１～Ｄ８をその番号順に一時記憶する。電文順序並替部１３は、分割された電文の総数を認識する。ここでは、分割された電文の総数が１６であることを認識する。電文順序並替部１３は、分割された電文の総数の範囲で乱数を順次発生し、発生した乱数に基づいて電文順序の並べ替えを行う。なお、電文順序並替部１３は、複数の並べ替え順序を予め備えており、その中からランダムに１つの並べ替え順序を抽出し、抽出した並べ替え順序に基づいて電文順序の並べ替えを行うようにしてもよい。電文順序の並べ替え結果の一例を図３（ｂ）に示す。

図４は、制御情報の例を示す図である。制御電文生成部１４は、電文順序の並べ替えの結果に基づいて並べ替えられた電文を元の順序に戻すための制御情報を生成する。図４（ａ）に示す制御情報は、並べ替えられた電文の順序を示すようにしたもので、０はダミー電文であることを、１～８は送信電文であることを示している。ここで、図４（ａ）は最初がダミー電文、２番目が分割された送信電文の７番目、３番目がダミー電文、４番目がダミー電文、５番目が分割された送信電文の５番目、……、最後が送信電文の６番目であることを示している。

図４（ｂ）に示す他の制御情報は、分割された送信電文の１番目（Ｓ１）が１２番目のパケットで送信され、分割された送信電文の２番目（Ｓ２）が７番目のパケットで送信され、分割された送信電文の３番目が９番目のパケットで送信され、……、分割された送信電文の８番目が１０番目のパケットで送信されることを示している。

なお、図４では、カンマ区切りの文字列からなる制御情報を例示したが、区切り記号は例えばスペース文字や／，＊，＋等の記号文字等の任意に記号を用いることができる。

図５は、データ送信部の動作を示す図である。データ送信部１５は、図３（ｂ）に示した並べ替え後の電文のそれぞれについてインターネットのプロトコルに対応したパケットにして、生成したパケットを順次送信する。具体的には、分割された電文（電文データ）の前にＴＣＰヘッダを付加し、さらにＴＣＰヘッダの前にＩＰヘッダを付加し、さらにその前にデータリンク層のヘッダを付加して送信する。ここで、データ送信部１５は、最初の電文Ｄ４を送信するパケットに対しては、ＴＣＰヘッダ内のシーケンスナンバー（何番目のパケットかを示す通し番号）を１とし、２番目の電文Ｓ７を送信するパケットに対しては、ＴＣＰヘッダ内のシーケンスナンバーを２とし、それ以降の各パケットに対して３，４，５，……のシーケンスナンバーをそれぞれ付けて送信する。また、データ送信部１５は、ＩＰヘッダ内の送信元ＩＰアドレスに本電文送信装置１０（電文送信側のコンピュータ）のＩＰアドレスを、ＩＰヘッダ内の宛先（送信先）ＩＰアドレスに送信先（電文受信装置２０を備える電文受信側のコンピュータ）のＩＰアドレスを付ける。

データ送信部１５は、分割された電文を全てパケット化して送信した後に、その通信を終了させる。そして、その後に電文受信装置２０との通信を再度開始する要求を発生し、制御電文生成部１４で生成した制御電文をパケット化して送信する。なお、データ送信部１５は、分割された電文を全てパケット化して送信した直後に、その通信を終了させることなく、制御電文をパケット化して送信するようにしてもよい。

なお、データ送信部１５とデータ受信部２１との間では、パケットの到着確認処理やパケットが正常に到着できなかったときの再送信処理等がなされる。なお、これらの処理等はＴＣＰプロトコル及びＩＰプロトコルで規定されている。

電文受信装置２０側のデータ受信部２１は、受信したパケットが電文パケットである場合は、その電文パケット中の電文を受信電文記憶部２

２へ供給し、受信したパケットが制御パケットである場合は、その制御パケット中の制御情報（制御電文）を制御電文記憶部２３へ供給する。

なお、データ受信部２１は受信したパケットのデータに基づいて電文であるか制御情報であるかを判断するようにしている。具体的には、受信したデータが区切り文字等で区切られたデータである場合は制御情報と判断し、それ以外は電文であると判断する。なお、複数のパケットから構成されている場合には電文であると判断し、単一のパケットのみである場合には制御情報と判断するようにしてもよい。また、データ送信部１５側でＴＣＰヘッダ内に電文と制御情報とを区別する情報を挿入して送信し、データ受信部２１はＴＣＰヘッダ内に挿入された情報に基づいて電文と制御情報とを判別するようにしてもよい。また、データ送信部１５側で制御パケットを送信する際には、データ部に制御情報であることを示す情報を挿入しておき、データ受信部２１はデータ部内に制御情報であることを示す情報が挿入されているか否かに基づいて電文であるか制御情報であるかを判断するようにしてもよい。

受信した電文データは、そのパケットのシーケンスナンバー（何番目のパケットかを示す通し番号）との対応を付けて受信電文記憶部２２に一時記憶される。また、受信した制御情報は制御電文記憶部２３に一時記憶される。

図６は、電文復元部の動作を示す図である。電文復元部２４は、制御電文記憶部２３に記憶された制御情報に基づいて受信電文記憶部２２に記憶された電文を抽出して受信電文を復元する。具体的には、図６（ａ）に示す受信電文記憶部２２に記憶された電文の中から制御情報に基づいて分割された電文の第１番目を取り出し、次に分割された電文の第２番目，第３番目，……を順次取り出し、取り出した順に各電文を連結することで、図６（ｂ）に示すように、分割される前の電文（送信電文）を復元する。

本発明に係る電文送信装置は、電文を分割しその順序を並べ替えているだけであるので、インターネット３０上を伝送されるデータは断片化されているとはいえ平文である。しかしながら、有意な送信電文とダミ

一電文とが混在されて断片化されているので、インターネット３０上を伝送されるデータを盗聴したとしても、送信電文の内容を把握することは困難である。さらに、ダミー電文の内容を工夫することで、送信電文の内容把握をさらに困難にすることができる。例えば、本来の送信電文の内容が例えば「甲案に賛成」であった場合、ダミー電文の内容を「乙案に賛成」としたり、「甲案に反対」としたりすることで、第三者による内容の把握をさらに困難にすることができる。なお、ダミー電文は送信者が自ら作成してもよいし、コンピュータを利用してダミー電文を自動的に生成するようにしてもよい。

図１では、電文送信装置１０側で分割した電文をランダムに並べ替え、その並べ替え順序に関する制御情報を制御電文（制御パケット）として送信する構成を示したが、送信側と受信側とで予め並べ替える順序を定めている場合は、制御電文（制御パケット）の送受は不要となる。この場合は、制御電文生成部１４及び制御電文記憶部２３を設ける必要がない。　本発明では、制御パケットを開かない限り分割された電文を復元する順序を確定できない。したがって、制御パケットの経路履歴や開封確認をチェックすれば、送信内容を第三者に正確に把握されることを防止できる。そこで、制御パケットが各ルータを通過する際に、そのルータを特定するための情報（例えばルータのＵＲＬ）が制御パケットに追加記録されるようにすることで、制御パケットがどのような経路を経て受信側へ到達したかの経路ログを得ることができる。さらに、制御パケットが開封された際に開封された旨の情報が制御パケットに記録され、制御パケットが複製された際に複製された旨の情報が制御パケットに記録されるようにすることで、制御パケットを受信した時点で何らかの不正アクセスがあったか否かを特定することが可能となる。そして、電文受信装置２０は、途中で開封された旨の記録があるパケットを受信した場合には、その旨を電文送信装置１０側に通知し、受信電文を廃棄することで正常でない電文を復元するおそれをなくすことができる。　以上説明したように本発明は、送信側において送信電文及びダミー電文を分割しそれらの順序を並べ替えて送信するので、断片化されかつダミー

の電文が含まれているため、電文が盗聴等された場合でも電文内容を正確に把握するのが困難である。本発明は、共通鍵方式や公開鍵方式等の暗号化処理／復号化処理を一切用いていないので、送信側及び受信側の構成及びデータ処理を簡易なものにすることができる。

本明細書で引用した全ての刊行物、特許および特許出願をそのまま参考として本明細書にとり入れるものとする。

産業上の利用の可能性

本発明は電文送受信の機密性を高めるのに有用である。

請　求　の　範　囲

1．　送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文をパケット通信方式で送信するデータ送信部と、を備えることを特徴とする電文送信装置。

2．　送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文を元の順序に戻すための制御情報を有する制御電文を生成する制御電文生成部と、前記電文順序並替部によって並べ替えられた送信電文及び前記制御電文生成部によって生成された制御電文をパケット通信方式で送信するデータ送信部と、を備えることを特徴とする電文送信装置。

3．　前記データ送信部は、前記電文順序並替部によって並べ替えられた送信電文と前記制御電文とを別に送信することを特徴とする請求項2記載の電文送信装置。

4．　前記ダミー電文は、前記送信電文の内容と異なる内容であって、送信電文の内容の把握を妨げる内容であることを特徴とする請求項1又は2記載の電文送信装置。

5．　パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した電文を記憶する受信電文記憶部と、該受信電文記憶部に記憶されている電文からダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備えることを特徴とする電文受信装置。

6．　パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した受信電文を記憶する受信電文記憶部と、該データ受信部で受信した制御電文を記憶する制御電文記憶部と、前記受信電文記憶部に記憶されている電文から前記制御電文記憶部に記憶されている制

御電文に基づいてダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備えることを特徴とする電文受信装置。

要　約　書

送信電文及びダミー電文をそれぞれ分割して混合しかつそれらの順序を入れ替えて伝送することで、盗聴等による電文内容の把握を困難にする。

電文送信装置１０は、送信電文を送信電文分割部１１で分割し、ダミー電文をダミー電文分割部１２で分割し、分割した各電文の順序を電文順序並替部１３で並べ替える。制御電文生成部１４は、並べ替えられた送信電文を元の順序に戻すための制御情報からなる制御電文を生成する。データ送信部１５は、並べ替えられた送信電文を１つ毎にパケット化し、パケット通し番号を付けて送信する。データ送信部１５は、送信電文とは別途に制御電文をパケット化して送信する。電文受信装置２０は、受信した電文をパケット通し番号との対応を付けて受信電文記憶部２２に格納する。電文復元部２４は、受信した制御情報に基づいて電文の順序を元に戻して連結することで、本来の送信電文を復元する。

図 1

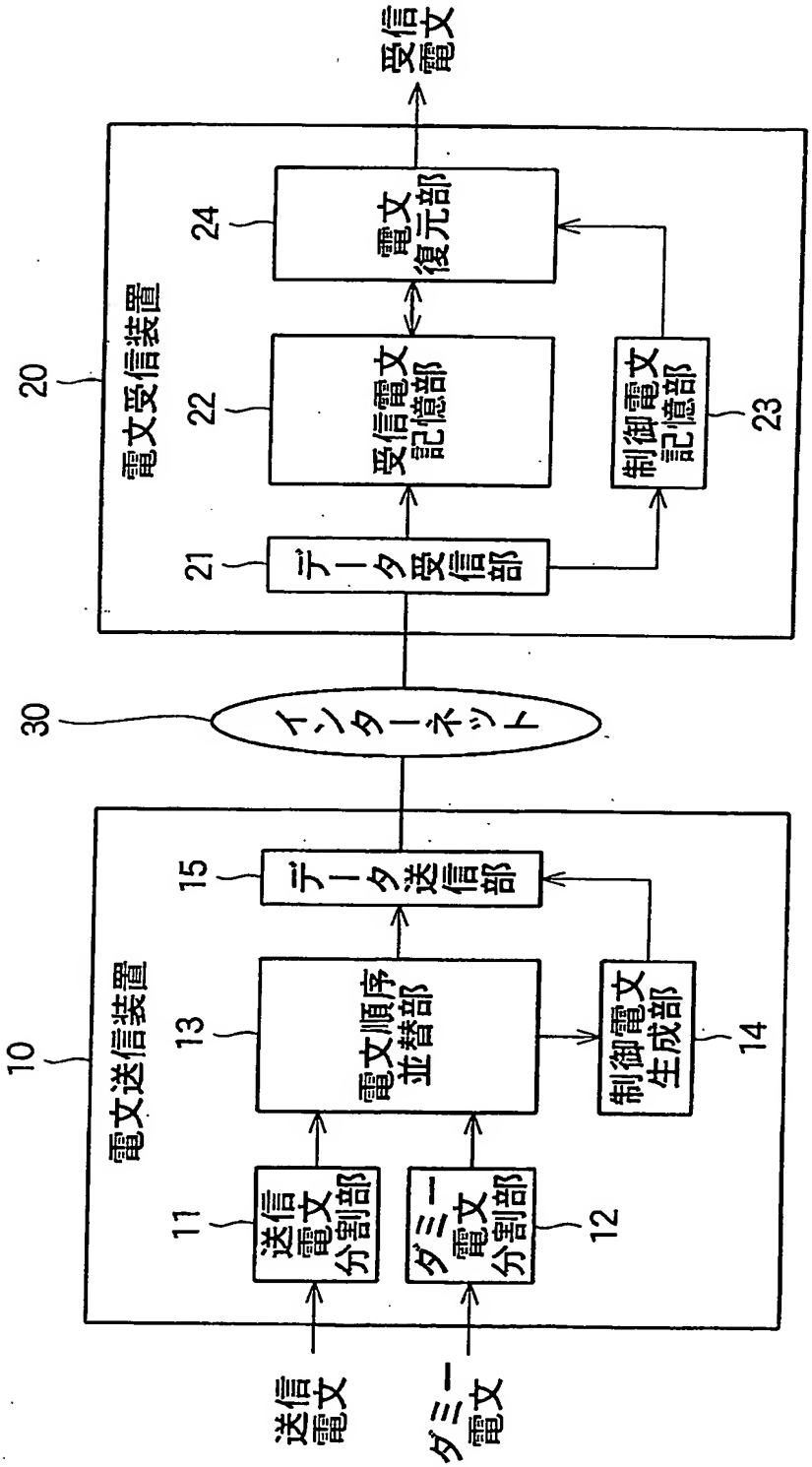
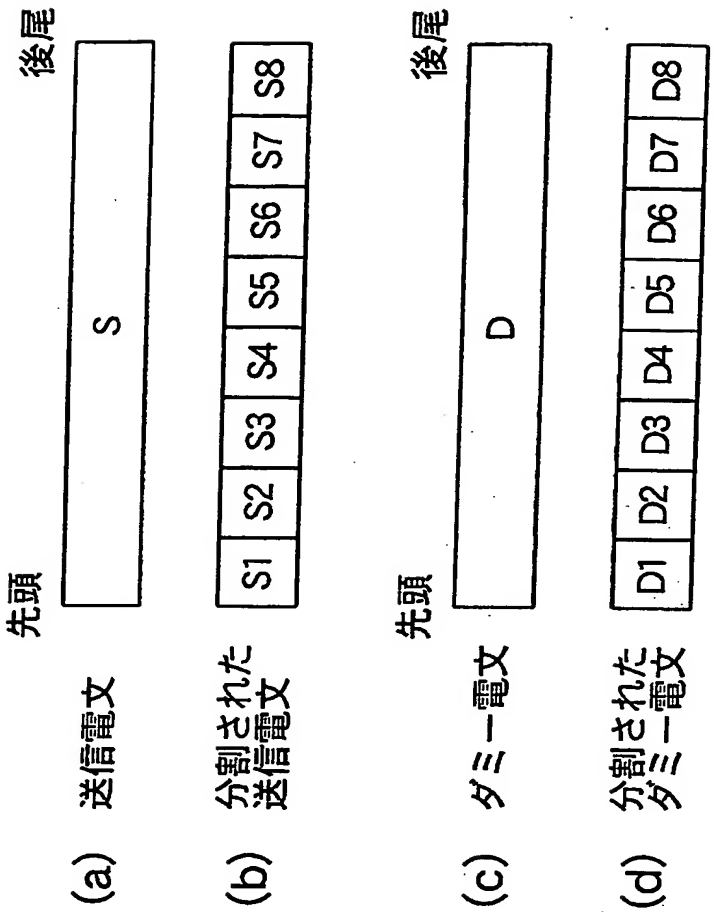
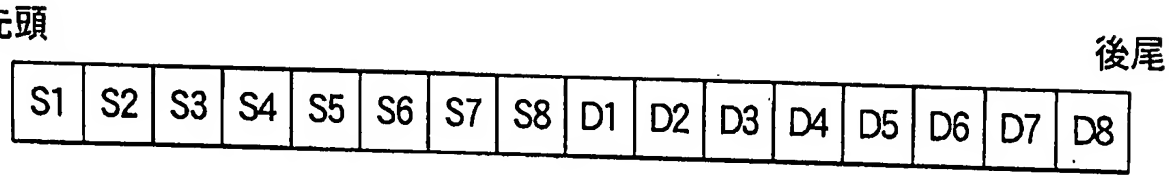

受信電文
電文受信装置
20
24
電文復元部
22
受信電文記憶部
23
制御電文記憶部
21
データ受信部
30
インターネット
電文送信装置
10
15
データ送信部
13
電文順序並替部
14
制御電文生成部
11
送信電文分割部
12
ダミー電文分割部
送信電文
ダミー電文

図 2


先頭
後尾
S
S1
S2
S3
S4
S5
S6
S7
S8
D
D1
D2
D3
D4
D5
D6
D7
D8
(a) 送信電文
(b) 分割された送信電文
(c) ダミー電文
(d) 分割されたダミー電文

(a) 並べ替え前の電文順序



(b) 並べ替え後の電文順序

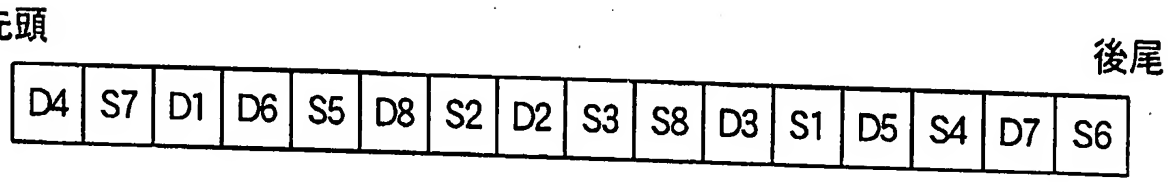


図3

(a) 制御情報(一例)

先頭　　後尾

0, 7, 0, 0, 5, 0, 2, 0, 3, 8, 0, 1, 0, 4, 0, 6

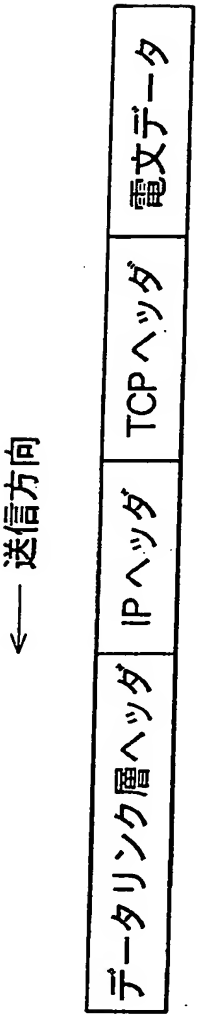
(b) 制御情報(他の例)

先頭　　後尾

12, 7, 9, 14, 5, 16, 2, 10

図4

図 5



(a) 受信した電文の順序

先頭　　後尾

パケット通し番号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	D4	S7	D1	D6	S5	D8	S2	D2	S3	S8	D3	S1	D5	S4	D7	S6

(b) 復元した受信電文(送信電文)

S1	S2	S3	S4	S5	S6	S7	S8

図6